MELINDA HAAG (CABN 132612)
United States Attorney

DAVID R. CALLAWAY (CABN 121782)
Chief, Criminal Division

BENJAMIN TOLKOFF (NYBN 4294443)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7200
FAX: (415) 436-7234
Benjamin.Tolkoff@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>Plaintiff,<br><br>v.<br><br>ELIJAH COOPER,<br><br>Defendant. | No. CR 13-693 SI<br><br>**ADDENDUM TO UNITED STATES' FILING OF JANUARY 30, 2015**<br><br>Date: February 6, 2015.<br>Time: 11:00 a.m. |

## I. INTRODUCTION:

There are two key issues before the Court: what showing the government must make to get historical cell site data; and what showing the government must make to get prospective or real-time cell site data.

As to the first issue, the law is fairly well settled. The government may obtain historical cell site data with an 18 U.S.C. § 2703(d) order.[1]

[1] *See, e.g., In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 306-308 (3d Cir. 2010); *In re U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *United States v. Graham*, 846 F.Supp.2d 384, 404 (D.Md.2012); *In re Application for an Order Authorizing the Release of Historical Cell–Site Information*, No. 11–MC–0113(JO), 2011 WL 679925, at *2 (E.D.N.Y. Feb.16, 2011); *United States v. Dye*, NO. 1:10CR221, 2011 WL 1595255, at *9 (N.D.Ohio Apr.27, 2011); *United States v. Velasquez*, No. CR08–0730 WHA,

> As to the second matter, the law is all over the map.
>
> Neither the Supreme Court nor the Ninth Circuit has addressed whether prospective or real-time CSLI is protected by the Fourth Amendment, *i.e.*, whether there is a reasonable expectation of privacy in such information. Even without addressing the Fourth Amendment issue, neither of these courts have addressed, as a matter of statutory construction, whether a warrant based on probable cause is required to obtain this information or if some lesser showing is sufficient. The decisions of other courts on this issue are not uniform. Some courts have found that this information is obtainable under the "specific and articulable facts" standard of the SCA combined with the "relevant to an ongoing criminal investigation" standard of the pen register/trap and trace provisions. Others have required a warrant based on probable cause. Still others have devised alternative standards. It is worth pointing out that most courts that have addressed the issue and determined that a warrant and probable cause are required have not made the determination under the Fourth Amendment, but instead find that there is no other statutory authority under which to authorize the disclosure of the information.

*Meisler v. Chrzanowski*, No. 3:12-CV-00487-MMD, 2013 WL 5375524, at *12 (D. Nev. Sept. 24, 2013).

In its research, the government found more than eighty cases on the matter, mostly from magistrate and district court judges. *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012), concluded that there is no Fourth Amendment expectation of privacy in signals emitted from a cell phone, including real-time GPS signals. Of course, *Skinner* is not binding on this Court.

Judge Huvelle of the District of D.C. may have said it best when she reasoned:

> [T]here is a robust debate over the question of whether the Fourth Amendment applies to cell-site data obtained from a cellular provider, but to date, this Court knows of no federal court that has held that the use of *prospective* cell-site records constitutes a search under the Fourth Amendment, or of any federal court that has suppressed any type of cell-site data obtained pursuant to a court order under the SCA.

*United States v. Jones*, 908 F. Supp. 2d 203, 213 (D.D.C. 2012)(emphasis in original).

Some Courts hold that the government can get prospective cell site records with a 2703(d) order, others hold that the government needs a warrant. But none of the Courts that required the government to get a warrant for the records has suppressed cell site data obtained in good faith reliance on a 2703(d) order. Therefore, even if this Court were to find a warrant requirement for cell site records, the remedy would not be suppression. For that reason, and for all other reasons previously raised during the course of litigation, Mr. Cooper's motion must be denied.

---

2010 WL 4286276, at *4–6 (N.D.Cal. Oct.22, 2010); *United States v. Benford*, No. 2:09 CR 86, 2010 WL 1266507, at *2–3 (N.D.Ind. Mar.26, 2010); *Suarez–Blanca*, 2008 WL 4200156, at *8; *In re Applications of the U.S. for Orders Pursuant to 18 U.S.C. § 2703(d)*, 509 F.Supp.2d 76, 80–81 (D.Mass.2007).

The government submits this pleading to lay out the state of the law on this issue.

**II. DISCUSSION:**

a. Circuit Court Cases:

The following are the appellate court opinions that either directly or indirectly bear on the issue.

1. Third Circuit:

*In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010) (Sloviter Opinion).

The Third Circuit addressed the denial of an application for order authorizing the disclosure of historical cell site data under § 2703(d). The court held:

> In sum, we hold that CSLI from cell phone calls is obtainable under a § 2703(d) order and that such an order does not require the traditional probable cause determination. Instead, the standard is governed by the text of § 2703(d), i.e., "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

*Id*. at 313.

The Third Circuit went on to comment that a magistrate may, in her discretion require the government to get a warrant for cell site data.

> Because the statute as presently written gives the MJ the option to require a warrant showing probable cause, we are unwilling to remove that option although it is an option to be used sparingly because Congress also included the option of a § 2703(d) order. However, should the MJ conclude that a warrant is required rather than a § 2703(d) order, on remand it is imperative that the MJ make fact findings and give a full explanation that balances the Government's need (not merely desire) for the information with the privacy interests of cell phone users.

*Id*. at 319.[2]

2. Fifth Circuit:

i. *In re U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013).

The Fifth Circuit addressed the narrow question of whether there was a Fourth Amendment

[2] It bears noting that Judge Tashima – Senior Judge of the Ninth Circuit did not join this latter portion of the Sloviter opinion and took issue with the majority's view that cell site data was not voluntarily shared with a third party. Tashima reasoned that there was no basis to conclude that cell site data is protected by the Fourth Amendment in light of *Smith v. Maryland*, 442 U.S. 735 (1979). *Id*. at 320-321.

expectation of privacy in historical cell site data. The court held:

> Cell site data are business records and should be analyzed under that line of Supreme Court precedent. Because the magistrate judge and district court treated the data as tracking information, they applied the wrong legal standard. Using the proper framework, the SCA's authorization of § 2703(d) orders for historical cell site information if an application meets the lesser "specific and articulable facts" standard, rather than the Fourth Amendment probable cause standard, is not per se unconstitutional.

*Id*. at 615.

The Fifth Circuit specifically rejected the Third Circuit's opinion that a magistrate judge could, at her discretion, require the government to get a warrant for cell site data, holding that the terms of § 2703 required the magistrate to issue an order when the government met its burden of specific and articulable facts. *Id*. at 607-608.

ii. *United States v. Guerrero*, 768 F.3d 351 (5th Cir. 2014).

Defendant Guerrero challenged the admission at trial of his cell site records. The government conceded that the process required under the Stored Communications Act was not followed (they had been obtained with a subpoena, not a § 2703(d) order). The Fifth Circuit held that, even though the SCA was violated, the records were properly admitted.

> For Guerrero to suppress the cell site location data, he therefore must show that the cell site location data was obtained not just in violation of the Act, but also in violation of the Fourth Amendment. That constitutional question requires a separate inquiry, and it is one we recently addressed. In *Historical Cell Site*, we held that "Section 2703(d) orders to obtain historical cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional." 724 F.3d at 615. We emphasized that cell phone users voluntarily convey information to their service providers and reasoned that they "understand that their service providers record their location information when they use their phones at least to the same extent that the landline users in *Smith* [*v. Maryland*, 442 U.S. 735, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979)] understood that the phone company recorded the numbers they dialed." *Id*. at 613. Although our holding in Historical Cell Site was decided only in the context of reviewing the denial of applications for Section 2703(d) orders, it nonetheless encompasses the exact issue before us now: whether historical cell site information—that is, a record that the "provider has already created"—is subject to a reasonable expectation of privacy that implicates the Fourth Amendment. *Id*. at 612; see id. at 615.

*Guerrero* at 358-359.

3. Sixth Circuit:

*United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012).

The government used cell site data and GPS data emanating from defendant's phone to establish his location as he transported drugs along public roads across state lines. *Id*. at 774.

> There is no Fourth Amendment violation because Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone. If a tool used to transport contraband gives off a signal that can be tracked for location, certainly the police can track the signal. The law cannot be that a criminal is entitled to rely on the expected untrackability of his tools. Otherwise, dogs could not be used to track a fugitive if the fugitive did not know that the dog hounds had his scent. A getaway car could not be identified and followed based on the license plate number if the driver reasonably thought he had gotten away unseen. The recent nature of cell phone location technology does not change this. If it did, then technology would help criminals but not the police. It follows that Skinner had no expectation of privacy in the context of this case, just as the driver of a getaway car has no expectation of privacy in the particular combination of colors of the car's paint.

*Id*. at 777.

The *Skinner* Court went on to clarify:

> We do not mean to suggest that there was no reasonable expectation of privacy because Skinner's phone was used in the commission of a crime, or that the cell phone was illegally possessed. On the contrary, an innocent actor would similarly lack a reasonable expectation of privacy in the inherent external locatability of a tool that he or she bought.

*Id.* at 777, footnote 1.

4. Seventh Circuit:

*United States v. Thousand*, 558 F. App'x 666 (7th Cir. 2014).

Affirming the denial of a motion to suppress and *Franks* hearing, the Seventh Circuit did not directly address the issue of what process was required to authorize the seizure of cell site location information, historical or prospective, but did telegraph its views on the matter.

> Before the days of mobile phones, the Supreme Court held that a person has no legitimate expectation of privacy in a phone company's records of numbers dialed on a telephone, and thus a defendant cannot invoke the Fourth Amendment when the police install a pen register without a warrant. *Smith v. Maryland*, 442 U.S. 735, 745–46, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979); *see United States v. Kramer*, 711 F.2d 789, 792 (7th Cir.1983). After *Smith* was decided, Congress enacted the Electronic Communications Privacy Act of 1986, Pub.L. No. 99–508, 100 Stat. 1848 We have yet to address whether, notwithstanding *Smith*, cell-tower information that telecommunication carriers collect is protected by the Fourth Amendment. Recently the Fifth Circuit concluded that Supreme Court precedent "does not recognize a situation where a conventional order for a third party's voluntarily created business records transforms into a Fourth Amendment search or seizure," and thus the court rejected the contention that using court

> orders available through the Stored Communications Act to collect historical cell-tower data without a showing of probable cause is unconstitutional. *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600, 614–15 (5th Cir.2013); *see also In re Application of U.S. for Order Directing Provider of Elec. Commc'n, Serv. to Disclose Records to Gov't*, 620 F.3d at 313–15 (concluding that, although § 2703(d) does not require authorities to show probable cause to obtain historical cell-tower data, judges have authority in particular cases to reject § 2703(d) applications and instead require use of search warrant establishing probable cause); *United States v. Forest*, 355 F.3d 942, 950–52 (6th Cir.2004) (concluding that DEA use of cell-site data was not a "search" under Fourth Amendment because authorities tracked defendant's movements along public highways), *vacated on other grounds sub. nom. Garner v. United States*, 543 U.S. 1100, 125 S.Ct. 1050, 160 L.Ed.2d 1001 (2005). **We have not found any federal appellate decision accepting Thousand's premise that obtaining cell-site data from telecommunications companies—under any factual scenario—raises a concern under the Fourth Amendment**.

*Thousand*, at 670. (Emphasis added)

b. District Court Cases:

There are dozens of district court cases that address what the government must do to get cell site data. The opinions cited below give a fulsome and well-reasoned analysis.

1. *United States v. Banks*, No. 13-CR-40060-DDC, 2014 WL 4594197 (D. Kan. Sept. 15, 2014). In the context of historical cell site data, the District of Kansas held that there was no Fourth Amendment expectation of privacy in cell site data.

> The cell service provider collects and stores historical cell site data for its own business purposes, perhaps to monitor or optimize service on its network or to accurately bill its customers for the segments of its network that they use. Under this framework, cell site information is clearly a business record. Analyzed as a business record, a conveyance of location information to the service provider nevertheless must be voluntary in order for the cell phone owner to relinquish his privacy interest in the data. The Court finds that such conveyances are in fact, voluntary. A cell service subscriber, like a telephone user, understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call. Even if this cell phone-to-tower signal transmission was not 'common knowledge,' " cell service providers adopt contractual privacy policies and terms of use that "expressly state that a provider uses a subscriber's location information to route his cell phone calls. These policies inform users that providers not only use CSLI, but also collect and record it. Although the defendants may *prefer* their location information to remain private, the Court does not believe that defendants reasonably could expect privacy because they voluntarily conveyed the information to third parties who openly collected and recorded it. . .
> Because the defendants voluntarily conveyed CSLI to service providers as part of a business transaction, the statutory standard in 2703(d) governs and Fourth Amendment protections do not apply to their CSLI.

*Id*. at *4.

2. *United States v. Caraballo*, 963 F. Supp. 2d 341, 359-60 (D. Vt. 2013)

Citing Judge Brown of the Eastern District of New York (infra) and the Sixth Circuit's *Skinner* decision (supra), the District of Vermont denied defendant's motion to suppress holding that he had no expectation of privacy in his real-time cell site data.

> [A]ll the known tracking technologies may be defeated by merely turning off the phone . . . [I]ndividuals who do not want to be disturbed by unwanted telephone calls at a particular time or place simply turn their phones off, knowing that they cannot be located.
> . . .
> Accordingly, as a general proposition, cell phone location data is information a cell phone user voluntarily discloses to a third party in order to enable the cell phone user to send and receive calls. *Smith* and *Miller* thus support a conclusion that a cell phone user generally has no reasonable expectation of privacy in cell site information communicated for the purpose or making and receiving calls in the ordinary course of the provision of cellular phone service.

*Id*. at 359-60. (Internal citations and quotations omitted).

3. *In re Smartphone Geolocation Data Application*, 977 F. Supp. 2d 129 (E.D.N.Y. 2013)(Brown Opinion). In the context of an application for geolocation data for a fugitive, Judge Brown gave what the government has found to be the most thorough and accurate assessment of the technology at issue and the state of the law. He held that the government could get geolocation data with a § 2703(d) order.[3]

> The Second Circuit has not ruled directly on the question of whether a user has a reasonable expectation of privacy in geolocation data, though it has supplied some guidance on the question. In *United States v. Pascual*, 502 Fed.Appx. 75 (2d Cir.2012), the defendant argued that "the district court improperly admitted cell-site records secured pursuant to a subpoena, without a warrant or a showing of probable cause." *Id.* at 80. Because the defendant failed to preserve the issue, it was reviewed for plain error. The Circuit observed that the defendant's position was "(at the very least) in some tension with prevailing case law," citing *Smith v. Maryland*, 442 U.S. 735, 742–44, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979) (a customer has no reasonable expectation of privacy in dialed phone number conveyed to telephone company), and *United States v. Miller*, 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976) (Fourth Amendment inapplicable to information conveyed to a third party).
> . . .

[3] Geolocation including GPS and E-911 data can pinpoint the location of a device. Cell site data cannot.

> It is clearly within the knowledge of cell phone users that their telecommunication carrier, smartphone manufacturer and others are aware of the location of their cell phone at any given time . . .
> Conversely, individuals who do not want to be disturbed by unwanted telephone calls at a particular time or place simply turn their phones off, knowing that they cannot be located.
> . . .
> A central element in determining whether an individual has a reasonable expectation of privacy is the effort made to keep the subject information private.
> . . .
> [A] cell phone user such as the defendant can easily protect the privacy of location data—literally at the touch of a button—and should not be heard to complain if he fails to do so.
> . . .
> Thus, it would appear that the Government may obtain prospective cell site authorization either by securing a search warrant or an order under § 2703(d).
> . . .
> Construing "tracking device" to encompass a cell phone is simply illogical and unworkable in this context. For example, under the broader reading, an individual travelling by bicycle, leaving tire tracks in a muddy field; an automobile taillight, which could permit officers to follow a car at night; or the transmitter of a pirate radio station, the signal from which may be located via triangulation, would each constitute an "electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b). That officials opt to follow these clues could not possibly transform the bicycle, taillight or illegal transmitter into a tracking device requiring a search warrant, and such an interpretation would do violence to the clear intent of the statute. Similarly, I find that gathering geolocation information about a cellular telephone does not convert the phone into a "tracking device" for the purpose of the statute.
> . . .
> Thus, because a cell phone does not fall within the "tracking device" exclusion, the Government may properly seek an authorization order for prospective cell site data under section 2703.

*Id*. at 143-50. (Internal citations and quotations omitted).

4. *In re Applications of U.S. for Orders Pursuant to Title 18, U.S.Code Section 2703(d)*, 509 F. Supp. 2d 76 (D. Mass. 2007).

The District of Massachusetts, addressing an application for historical cell site data raised a real question of any Fourth Amendment interest in cell site data.

> [I]f an order requiring the disclosure of prospective cell site information allowed the government to "track" a suspect (or more accurately his or her phone) into a protected area like a home, would any reasonable Fourth Amendment expectation of privacy be compromised as a result? Unlike *United States v. Karo*, 468 U.S. 705, 715, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984), where the electronic beeper concealed in the drum of ether disclosed not only the location of defendant's home, but also the fact that criminal activity was afoot (which featured prominently in the search warrant affidavit), there is nothing presumptively illegal about the possession of a cellular phone. The most that the "tracked" cell phone might reveal is that its owner might presently be found in the home (assuming that the phone had not been loaned to someone else). There is nothing, however, about that disclosure that is any more incriminating or revealing than

> what could be gleaned from the activation of a pen register or from physical surveillance. Moreover, outside of the home it is doubtful that the tracking of a cell phone has any Fourth Amendment implication whatsoever.

*Id*. at 81.

5. *In re Application for an Order Authorizing The Extension and use of a Pen Register Device, etc*. 2007 WL 397129 (E.D.Cal., 2007) (Hollows Opinion).

Judge Hollows authorized an application for real-time cell site data finding:

> it would prove far too much to find that Congress contemplated legislating about cell phones as tracking devices. For example, if an agent presently used a cell phone to communicate the whereabouts of a suspect by using the phone's video feature while he was surveilling the suspect, one could fit this situation into the words of the statute-one was using an electronic device which "permitted" the tracking of the suspect. Or, take the example of the ubiquitous monitoring cameras, such as the "red light," parking lot or freeway cameras. These cameras track the location of many persons, albeit in a confined location, and could also fit in with the words of the statute. It is best to take the cue from Congress in this respect of electronic tracking devices, and confine § 3117(b) to the transponder type devices placed upon the object or person to be tracked. The court need not reach the situation where the target was using his or her cell phone within the confines of a home. However, suffice it to say that the only apparent electronic tracking performed in such a case is all done outside the home via cell towers. Unless the agents are calling the suspect's phone, the agents have no control over the suspect's use of the cell phone whatever in his location, did not cause or initiate the cell phone signal, and are not keying in on the cell phone signal *inside the home.* Mathematical triangulations made from different cell phone towers outside the home which will reveal a general area where the suspect may be found is hardly probing inside the house.

*Id.* at *2, footnote 2.

6. *In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d 448 (S.D.N.Y. 2006)(Kaplan Opinion).

Granting an application for prospective cell site data, Judge Kaplan held:

> The Stored Communications Act contains no explicit limitation on the disclosure of prospective data. Further, the information the government requests is, in fact, a stored, historical record because it will be received by the cell phone service provider and stored, if only momentarily, before being forwarded to law enforcement officials.
> …
> Accordingly, because a cell phone provider is an "electronic communications service" and cell site information is a "record or other information pertaining to a subscriber to or a customer of" the cell phone provider, the logical conclusion is that Sections 2703(c) and (d) permit a court to order the disclosure of prospective cell site information upon a proper showing by the government.

*Id.* at 459-461.

7. *In re Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Information,* 433 F.Supp.2d 804 (S.D.Tex.2006)(Rosenthal Opinion).

Under circumstances nearly identical to those here, Judge Rosenthal, citing the Kaplan and Gorenstein Opinions (infra), granted applications for § 2703(d) orders authorizing the government to obtain the exact data the government has obtained here.

> First, the cell site information provided in this District is tied only to telephone calls actually made or received by the telephone user. Thus, no data is provided as to the location of the cell phone when no call is in progress. Second, at any given moment, data is provided only as to a single cell tower with which the cell phone is communicating. Thus, no data is provided that could be "triangulated" to permit the precise location of the cell phone user. Third, the data is not obtained by the Government directly but is instead transmitted from the provider digitally to a computer maintained by the Government.
> . . .
> The government is not seeking: (1) to activate remotely the subject telephone's GPS functionality; (2) to obtain information from multiple cellular antenna towers simultaneously to "triangulate" the precise location of a cell phone; or (3) to place calls to a particular cell phone repeatedly or otherwise to track on a continuous basis the location of a cell phone when no call is being placed or received. Instead, the government seeks an order to install a pen register/trap and trace device configured to provide cell-site information at the origin and termination of calls and, if reasonably available, during the progress of a call that is not initiated by the government itself.

*Id*. at 806.

8. *In re Application of U.S. for an Order for Disclosure of Telecommunications Records & Authorizing the Use of a Pen Register & Trap & Trace*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) (Gorenstein Opinion).

> We next turn back to section 2703, which governs "information" pertaining to "customers and users" of electronic communications service. It is certainly the case that cell site or tracking information constitutes "information" pertaining to customers or users of electronic communications services. Thus, such cell site or tracking information comes within section 2703(c) and consequently is the sort of "information" that the Government may seek pursuant to an order under section 2703(d).

*Id*. at 445.

c. Good Faith:

The fatal problem with the defendant's motion is that all of the cases on which he relies were in a different posture. The government had applied for orders to get cell site data and the court denied the application. There is no case to which the defendant can point that stands for the proposition that

records, obtained in good faith with a § 2703(d) order should be suppressed. In fact, the cases that have addressed the issue have all held that the good faith doctrine applies and suppression is not warranted.

1. *United States v. Jones*, 908 F. Supp. 2d 203, 209 (D.D.C. 2012)

> All courts that have addressed the issue have held that the SCA does not provide for a suppression remedy. *See, e.g., United States v. Ferguson,* 508 F.Supp.2d 7, 10 (D.D.C.2007); *United States v. Hardrick,* 2012 WL 4883666, at *8 n. 44 (E.D.La. Oct. 15, 2012) (collecting cases). Section 2708 of the SCA provides that "[t]he remedies and sanctions described in this chapter are the *only* judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708 (emphasis added). Elsewhere, the Act provides for civil damages, *see id.* § 2707, and criminal penalties, *see id.* § 2701(b), but nowhere does it provide for the suppression of evidence. *See United States v. Smith,* 155 F.3d 1051, 1056 (9th Cir.1998) ("[T]he Stored Communications Act does *not* provide an exclusion remedy.").

*Id*. at 209.

> this Court knows of no . . . federal court that has suppressed any type of cell-site data obtained pursuant to a court order under the SCA.

*Id*. at 213.

2. *United States v. Hardrick*, No. CRIM.A. 10-202, 2012 WL 4883666, (E.D. La. Oct. 15, 2012)

> Because this Court holds that the good-faith exception to the exclusionary rule applies, *see* discussion *infra,* this Court need not reach the issue of whether the obtaining of CSLI is a Fourth Amendment search. *See United States v. Allen,* 625 F.3d 830, 835 (5th Cir.2010) ("First, we ask whether the seizure falls within the good-faith exception to the exclusionary rule ... [i]f the good-faith exception applies, this court affirms the district court's decision denying the motion to suppress."); *United States v. Craig,* 861 F.2d 818, 820 (5th Cir.1988)("Principles of judicial restraint and precedent dictate that, in most cases, we should not reach the probable cause issue if a decision on the admissibility of the evidence under the good-faith exception of *Leon* will resolve the matter."); *United States v. Cherna,* 184 F.3d 403, 407 (5th Cir.1999)("If the good-faith exception applies, we need not reach the question of probable cause."); *see also United States v. Webb,* 255 F.3d 890, 904–05 (D.C.Cir.2001) (holding that the good-faith exception applied no matter "what may be said of the search warrant affidavit in this case"); *Ferguson,* 508 F.Supp.2d at 10 (declining to address a Fourth Amendment challenge after holding that the good-faith exception applied); *United States v. Koch,* 625 F.3d 470, 476–77 (8th Cir.2010)("We need not address [whether there was a Fourth Amendment violation] because we conclude that the agents had an objective good faith belief ... that their search was legal.").

*Id*. at *4.

3. *United States v. Espudo,* 954 F. Supp. 2d 1029 (S.D. Cal. 2013)

Mr. Balogh cites *Espudo* for the proposition that the government cannot obtain prospective cell site data with a § 2703(d) order. He is right. But what Balogh fails to mention is that Judge Gonzalez refused to suppress cell site data obtained in good faith reliance on a § 2703(d) order.

> Starting from the premise that the exclusionary rule is a judicially created remedy, the Supreme Court created a good faith exception to the application of the exclusionary rule in *United States v. Leon*, 468 U.S. 897 (1984). Under this exception, the exclusionary rule does not bar the government's introduction of evidence obtained by officers acting in objectively reasonable reliance on a search warrant that is subsequently invalidated.
> In this case, the Government's reliance on the SCA and the Magistrate Judges' orders granting the applications was objectively reasonable. First, the Government's reliance on the SCA was reasonable. Acts of Congress are entitled to a strong presumption of constitutionality. It was reasonable for the Government to apply for cell site location data under the SCA. There is no clear, controlling case explicitly stating that the government may not obtain real-time cell site location data under the SCA. At most, there are only conflicting district court decisions on the subject.

*Id*. at 1044.

III. CONCLUSION:

There is no case that supports the relief the defendant seeks. Even those cases that require the government to get a warrant for real-time cell site data do not hold that suppression is appropriate where the government has relied in good faith on a § 2703 order. The defendant's motion must therefore be denied.

Date: February 5, 2015.

MELINDA HAAG
United States Attorney

/s/

BENJAMIN TOLKOFF
Assistant United States Attorney